Araştırma Makalesi

KAOTİK SES ŞİFRELEME ARAŞTIRILMASI VE UYGULAMASI

Anıl Emre DURAK[†], Mustafa Cem KASAPBAŞI[††]

[†] İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Ana Bilim Dalı, İstanbul, Türkiye

[††] İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Ana Bilim Dalı, İstanbul, Türkiye

24tsib013@istanbulticaret.edu.tr, mckasapbasi@ticaret.edu.tr

0000-0001-7100-1332, 0000-0001-6444-6659

Atıf/Citation: Durak A. E., Kasapbaşı M. C., (2025) Kaotik Ses Şifreleme Araştırılması ve Uygulaması, İstanbul Ticaret Üniversitesi Teknoloji ve Uygulamalı Bilimler Dergisi, Cilt 8. No 1, sayfa 117-132 DOI: 10.56809/icujtas.1597765

ÖZET

Bu makale, ses dosyalarını güvence altına almak için geliştirilmiş yenilikçi bir kaotik akış şifreleme yöntemini tanıtmaktadır. Çalışma, lojistik haritalar ve bellek tabanlı rastgelelik mekanizmalarını birleştirerek, mevcut şifreleme yöntemlerine kıyasla daha yüksek güvenlik ve performans sağlayan bir algoritma önermektedir. Kaotik sistemlerin doğrusal olmayan dinamik yapıları ve başlangıç koşullarına duyarlılık özellikleri, veri güvenliğinde benzersiz avantajlar sunmaktadır. Çalışma kapsamında şifreleme algoritması, konuşma, müzik ve beyaz gürültüden oluşan 12 farklı ses dosyası üzerinde test edilmiş ve algoritmanın tutarlılığı ile rastgelelik düzeyi değerlendirilmiştir.

Test sonuçları, algoritmanın tepe sinyal-gürültü oranı (PSNR), entropi ve NIST (National Institute of Standards and Technology) rastgelelik testleri gibi metrikler açısından başarılı olduğunu göstermiştir. Ayrıca, standart sapma değerleri ile ölçüm sonuçlarındaki tutarlılık doğrulanmıştır. Analizler, şifreleme yöntemiyle elde edilen çıktıların yüksek rastgelelik seviyesine ve düşük korelasyon katsayısına sahip olduğunu ortaya koymuştur. Bunun yanı sıra, yöntem, post-kuantum kriptografisi bağlamında geniş anahtar uzayı (2^186) sayesinde kuantum sonrası güvenlik tehditlerine karşı güçlü bir direnç göstermiştir.

Önerilen yöntem, özellikle ses verilerinin güvenliği için modern bir çözüm sunmakla birlikte, düşük hesaplama maliyeti ve yüksek güvenlik seviyesi ile veri güvenliğinde yenilikçi bir yaklaşım olarak öne çıkmaktadır. Çalışmanın bulguları, kaos tabanlı şifreleme algoritmalarının, hem teorik hem de pratik güvenlik uygulamalarında etkili bir araç olduğunu doğrulamaktadır.

Anahtar Kelimeler: ses şifreleme, kaotik şifreleme, veri güvenliği, kuantum sonrası, National Institute of Standards and Technology testleri

CHAOTIC AUDIO RESEARCH AND APPLICATION

ABSTRACT

This paper introduces a novel chaotic stream encryption method developed for securing audio files. Chaotic systems offer significant advantages in encryption processes due to their sensitivity to initial conditions and nonlinear dynamic structures. Audio files encrypted using the proposed method were analyzed using PSNR, entropy, and NIST(National Institute of Standards and Technology) randomness tests. Additionally, the security of the encrypted audio data was evaluated through spectrogram analysis. The spectrogram analysis and National Institute of Standards and Technology randomness tests demonstrated the algorithm's strong potential resistance to post-quantum security threats.

Keywords: audio encryption, chaotic encryption, data security, post-quantum, national institute of standards and technology tests

Geliş/Received	:	**07.12.2024**
Gözden Geçirme/Revised	:	**16.01.2025**
Kabul/Accepted	:	**16.01.2025**

1. GİRİŞ

Kriptografi ve şifreleme yöntemleri, dijital çağda veri güvenliği sağlama noktasında kritik öneme sahiptir. Özellikle ses dosyaları gibi dijital içeriklerin korunması, yalnızca bireysel mahremiyetin değil, aynı zamanda iletişim güvenliğinin de temel taşlarından biri olmuştur. Geleneksel şifreleme yöntemleri, artan veri boyutları ve modern sistemlerin yüksek performans gereksinimleri karşısında yetersiz kalırken, kaotik sistemler, başlangıç koşullarına duyarlılıkları ve doğrusal olmayan dinamik yapılarıyla bu alanda yenilikçi ve etkili bir çözüm sunmaktadır.

Bu çalışmada, ses dosyalarının güvenliğini sağlamak amacıyla geliştirilen yeni bir kaotik akış şifreleme yöntemi tanıtılmaktadır. Geliştirilen algoritmanın etkinliği ve güvenliği, geniş bir analiz çerçevesinde değerlendirilmiştir. Tepe sinyal-gürültü oranı (PSNR), entropi analizleri ve Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology) tarafından önerilen rastgelelik testleri ile yapılan doğrulamalar, algoritmanın üstün performansını ortaya koymuştur. Ayrıca, şifrelenmiş ses dosyalarının spektrogram analizleri, şifreleme işleminin veri bütünlüğünü koruyarak yüksek bir güvenlik seviyesi sunduğunu göstermiştir.

Önerilen yöntemin 2^{186} bitlik geniş bir anahtar uzayı sayesinde, kuantum sonrası güvenlik tehditlerine karşı dayanıklı olduğu öngörülmektedir. Kaotik sistemlerin karmaşık dinamik yapıları, yalnızca mevcut tehditlere karşı değil, aynı zamanda gelecekte ortaya çıkabilecek risklere karşı da güçlü bir savunma mekanizması sunmaktadır. Bu sonuçlar, kaotik şifreleme yönteminin ses verilerinin güvenliği için etkili ve yenilikçi bir çözüm sunduğunu kanıtlamaktadır. Çalışmamız, hem akademik literatüre değerli bir katkı sağlamayı hem de endüstriyel uygulamalarda pratik bir çerçeve sunmayı hedeflemektedir.

.

2. LİTERATÜR ARAŞTIRMASI

Modern dünyada veri güvenliği, kriptografi ve şifreleme yöntemlerinin sürekli gelişimi ile sağlanmaktadır. Geleneksel şifreleme yöntemleri, büyük veri boyutları ve modern sistemlerin yüksek performans gereksinimlerini karşılamakta yetersiz kalabilmektedir. Bu bağlamda, kaotik sistemler, doğrusal olmayan dinamik yapıları ve başlangıç koşullarına duyarlılıkları sayesinde veri güvenliğinde yenilikçi bir çözüm sunmaktadır.

Kaotik sistemlerin kriptografideki rolü, karmaşık dinamik davranışları ve rastgelelik üretme kabiliyetleri sayesinde geniş bir araştırma alanı bulmuştur. Chen ve arkadaşlarının üç boyutlu kaotik "cat maps" üzerine yaptığı çalışmalar, bu sistemlerin güvenlik açısından nasıl kullanılabileceğini ortaya koymaktadır (Chen et al., 2004). Özellikle kaotik sistemlerin simetrik şifreleme algoritmalarında sağladığı rastgelelik, güvenlik protokollerini güçlendiren önemli bir faktördür. Ses verilerinin şifrelenmesinde kaotik sistemlerin etkisi, doğrusal olmayan dinamiklerin avantajlarından biri olarak öne çıkmaktadır.

Lorenz sistemi gibi kaos teorisine dayalı yaklaşımlar, ses ve görüntü verilerinin güvenliği için etkili yöntemler geliştirilmesine olanak tanımaktadır (Lorenz, 1963). Ayrıca, Shannon'un gizlilik sistemlerine dair teorileri (Shannon, 1949), kaos temelli algoritmaların teorik temelini oluşturmakta ve veri şifrelemede sağlam bir çerçeve sunmaktadır. Bu teorik çerçeve, kaotik sistemlerin veri güvenliğinde geleneksel yöntemlere kıyasla daha üstün performans sunmasını mümkün kılmaktadır.

Son yıllarda, kaotik sistemlerin veri güvenliğinde kullanımına yönelik önemli araştırmalar yapılmıştır. Örneğin, Liu ve arkadaşları (2019), kaotik haritaların hibrit sistemlerde nasıl uygulanabileceğini ve şifreleme hızını artırarak veri güvenliğini nasıl güçlendirdiğini göstermiştir. Ayrıca, Wang ve ekibi (2021), kaotik sistemlerin IoT cihazları için hafif şifreleme yöntemleri geliştirmede kullanılabileceğini vurgulamış ve bu sistemlerin sınırlı kaynaklara sahip cihazlarda etkili bir şekilde çalışabildiğini rapor etmiştir.

Yakın tarihte, Roy ve arkadaşları (2022), kaotik haritaların entropi değerlerini artırmak ve veri güvenliğini güçlendirmek için nasıl optimize edilebileceğine dair önemli bulgular sunmuştur. Bu çalışmada, entropi ve korelasyon katsayılarının, kaotik haritaların parametrelerinin dikkatli seçimi ile önemli ölçüde iyileştirilebileceği gösterilmiştir. Ali ve ekibi (2023) ise NIST testlerinde üstün performans gösteren bir kaos temelli şifreleme algoritması önererek, bu yöntemlerin modern veri güvenliği ihtiyaçlarını karşılayabileceğini belirtmiştir.

Kaotik sistemlerin veri güvenliği üzerindeki etkisini ölçmek için kullanılan NIST rastgelelik testleri, son yıllarda daha yaygın bir şekilde uygulanmaktadır. Zhang ve arkadaşları (2023), kaotik sistemlerin rastgelelik seviyesini ölçmek için NIST testlerini kullanmış ve bu sistemlerin yüksek rastgelelik seviyeleri sunduğunu rapor etmiştir. Aynı zamanda, bu testlerin kaotik sistemlerin doğrusal olmayan yapısını doğrulamak için güçlü bir araç olduğu belirtilmiştir. Bunun yanı sıra, kuantum hesaplamanın ortaya çıkardığı tehditler, kaotik sistemlerin post-kuantum

kriptografi için bir çözüm olup olamayacağını araştıran birçok çalışma başlatmıştır. Bernstein ve arkadaşları (2020), kaotik sistemlerin kuantum hesaplama karşısındaki potansiyel dayanıklılığını değerlendirmiş ve bu sistemlerin kuantum sonrası güvenlik için umut verici bir çözüm sunduğunu vurgulamıştır.

Kaotik sistemler, başlangıç koşullarına duyarlılıkları ve doğrusal olmayan yapıları sayesinde veri güvenliğinde kritik bir rol oynamaktadır. Özellikle, kaotik haritaların rastgelelik üretme kapasitesi, şifreleme algoritmalarında yüksek güvenlik ve performans sağlamaktadır. Son yıllarda yapılan çalışmalar, bu sistemlerin geleneksel şifreleme yöntemlerine kıyasla daha etkili olduğunu göstermiştir. Örneğin, kaotik sistemlerin kullanıldığı yöntemlerin düşük hesaplama maliyetleri ile büyük veri setlerinde bile hızlı sonuçlar üretebildiği vurgulanmaktadır. Bu, kaotik şifreleme algoritmalarının veri yoğun uygulamalar için neden tercih edildiğini açıklamaktadır.

Ayrıca, kaotik sistemler üzerine yapılan araştırmalar, farklı veri türlerinde (örneğin, ses, video ve görüntü) etkili sonuçlar verdiğini ortaya koymaktadır. Ses şifreleme alanında, kaotik sistemlerin sağladığı rastgelelik, hem veri gizliliğini hem de güvenilirliğini artırmaktadır. Özellikle, konuşma ve müzik gibi ses verilerinin korunmasında kaotik haritaların kullanılması, bu tür verilerin ele geçirilmesini zorlaştırmaktadır. Literatürde, bu sistemlerin entropi seviyelerini artırarak, saldırılara karşı daha dirençli bir yapı sunduğu belirtilmiştir.

Kaos teorisinin önemli bir avantajı, çok küçük değişikliklerin bile büyük sonuçlar doğurabilmesidir. Bu özellik, kaotik sistemlerin yüksek karmaşıklık ve rastgelelik gerektiren şifreleme algoritmalarında kullanımını cazip hale getirmektedir. Özellikle, lojistik harita gibi basit kaotik sistemlerin şifreleme algoritmalarına entegrasyonu, güvenlik seviyesini artırmakta ve sistemin tahmin edilebilirliğini azaltmaktadır. Bu da, saldırganların şifreleme algoritmasını çözmesini daha da zorlaştırmaktadır.

Günümüzde artan veri güvenliği gereksinimleri, kaotik sistemlerin kullanım alanlarını genişletmiştir. Örneğin, IoT (Nesnelerin İnterneti) cihazları gibi sınırlı kaynaklara sahip sistemlerde kaotik şifreleme algoritmaları etkili çözümler sunmaktadır. Bu sistemlerde düşük işlem gücü ve enerji tüketimi gereksinimlerini karşılayan kaotik algoritmalar, aynı zamanda yüksek güvenlik seviyeleri sağlamaktadır. Literatürde, IoT cihazları için optimize edilmiş kaotik sistemlerin uygulanabilirliği üzerine yapılan çalışmalar, bu alanın potansiyelini ortaya koymaktadır. Kaotik sistemlerin bir diğer önemli kullanım alanı ise post-kuantum kriptografidir. Kuantum bilgisayarların veri güvenliğine yönelik tehditleri arttıkça, kaos temelli sistemlerin kuantum sonrası güvenlik çözümleri sunma potansiyeli de dikkat çekmektedir. Bu sistemlerin doğrusal olmayan yapıları, kuantum algoritmalarının tahmin edemeyeceği rastgelelik seviyeleri üretebilmekte ve böylece kuantum saldırılarına karşı etkili bir savunma mekanizması oluşturmaktadır. Bu bağlamda, kaos temelli sistemlerin veri güvenliği alanındaki önemi her geçen gün artmaktadır.

Sonuç olarak, kaotik sistemler sadece mevcut güvenlik tehditlerine yanıt vermekle kalmamakta, aynı zamanda gelecekte ortaya çıkabilecek risklere karşı da dayanıklı bir altyapı sunmaktadır. Kaos teorisine dayalı yöntemlerin literatürdeki yeri giderek artarken, bu yöntemlerin veri güvenliğinde sağladığı yenilikçi çözümler hem akademik literatürde hem de pratik uygulamalarda büyük yankı bulmaktadır. Özellikle ses şifreleme alanındaki araştırmalar, bu teknolojinin veri güvenliği açısından ne kadar kritik olduğunu bir kez daha ortaya koymaktadır.

3. MATERYAL ve METOT

3.1. Kullanılan Yazılımlar ve Donanımlar

Bu çalışmada, ses dosyalarının şifrelenmesi ve güvenlik analizlerinin yapılması için çeşitli yazılımlar ve donanımlar kullanılmıştır.

Geliştirme Ortamı: C programlama dili kullanılarak kaotik akış şifreleme algoritması geliştirilmiştir. Bu algoritmanın implementasyonu için Visual Studio Code IDE'si ve GCC derleyicisi kullanılmıştır.

Ses Dosyaları: Testlerde kullanılan ses dosyaları, ".wav" formatında olup ortalama olarak 10.0MB büyüklüğündedir.

NIST STS Test Yazılımı: NIST'in (National Institute of Standards and Technology) rastgelelik test paketi (STS-2.1.2) kullanılarak şifrelenen dosyaların rastgelelik analizi yapılmıştır.

İstatiksel Analizler: PSNR(Peak Signal-to-Noise Ratio), entropi, spektrogram ve kolerasyon analizi hesaplamaları C dilinde yazılan fonksiyonlar ile icra edilmiştir.

*Donanım:*Tüm analizler ve hesaplamalar, Dell-Latitude 5521 modelinde 11. Nesil intel core i7 işlemci, 32.0GB RAM'e sahip bilgisayarı özellikleri ile icra edilmiştir.

3.2. Kaotik Akış Şifreleme Algoritması

Çalışmanın ana şifreleme algoritması, kaotik sistemler üzerine kuruludur. Kaotik sistemlerin doğrudan şifreleme algoritmalarına uygulanması, kaotik sistemlerin başlangıç koşullarına duyarlılığından dolayı güvenliği artırmaktadır.

Kaotik Harita: Çalışmada kullanılan kaotik harita lojistik harita fonksiyonudur.

$$x_{n+1} = r x_N (1 - \chi_n) \tag{1}$$

Denklem (1) de r kontrol parameteresi olup 3.996161616161616 olarak belirlenmiştir. Başlangıç değeri olan x_0 ise şifreleme anahtarı olarak kullanılmıştır.

Şifreleme Süreci: Kaotik harita, giriş ses dosyasındaki her bir baytı şifrelemek için kullanılmıştır. Her bir ses baytı, kaotik haritadan elde edilen bir bayt ile XOR işlemi yapılarak şifrelenmiştir. Ancak bu çalışmada temel XOR işlemi, bellek tabanlı bir yapı ile geliştirilmiştir:

Bellek Temelli Yapı: XOR işlemi sırasında, belirli bir pencere büyüklüğündeki (Windows_size=16) önceki şifrelenmiş baytlardan rastgele bir seçim yapılmıştır. Bu yöntem, rastgelelik düzeyini artırmak ve NIST Run Test gibi rastgelelik ölçütlerini iyileştirmek için kullanılmıştır.

```
// Şifreleme ve çözme işlemi
void chaotic_encrypt_decrypt(unsigned char* data, long length, double x0, double r, double y0, double rp) {
    long i;
    unsigned char window[WINDOW_SIZE] = { 0 };  // Pencere için bellek
    int window_index = 0;

    for (i = 0; i < length; i++) {
        x0 = logistic_map(x0, r);
        y0 = logistic_map(y0, rp);

        unsigned char chaotic_byte = (unsigned char)(fmod(x0 + y0, 1.0) * 255);

        // Bellekten rastgele seçim ve XOR işlemi
        unsigned char memory_byte = window[window_index];
        unsigned char enhanced_byte = chaotic_byte ^ memory_byte;

        data[i] ^= enhanced_byte;

        // Belleği güncelle
        window[window_index] = data[i];
        window_index = (window_index + 1) % WINDOW_SIZE;
    }
}
```

Şekil 1. Bellek Temelli Yapının proje içerisinde kullanımı gösterilmektedir.

Karmaşıklık Artışı: Bellek tabanlı rastgele seçim, şifreleme algoritmasının rastgelelik seviyesini ve güvenilirliğini artırmıştır.

3.3. Güvenlik Analizleri

Şifrelenen dosyaların güvenlik performansını değerlendirmek amacıyla birkaç temel test yapılmıştır:
PSNR (Peak Signal-to-Noise Ratio): Şifre çözme işleminden sonra orijinal ve deşifrelenmiş ses dosyaları arasındaki farkı ölçmek için PSNR hesaplanmıştır. PSNR değeri ne kadar yüksekse, şifre çözme işlemi o kadar başarılı sayılmaktadır. Aşağıda PSNR hesaplamak için kullanılan denklem (2) verilmiştir.

$$PSNR = 20 \cdot \log_{10} \left(\frac{MAX_I}{\sqrt{MSE}} \right) \tag{2}$$

Denklem(2)'de, MAX_I en yüksek sinyal değeri (örneğin, 8-bit veriler için 255) ve MSE ise ortalama kare hatasıdır.

Entropi Hesaplaması: Şifrelenen dosyaların entropi değerleri hesaplanarak, şifrelemenin ne kadar rastgele olduğu değerlendirilmiştir. Entropi, rastgeleliğin bir ölçüsü olarak kullanılır ve aşağıda gösterilen denklem (3) ile hesaplanır.

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log_2 p(x_i) \quad (3)$$

Denklem(3)'de, $p(x_i)$ herbir simgenin gerçekleşme olasılığıdır..

3.4. NIST Rastgelelik Testleri

Kaotik akış şifreleme algoritması ile şifrelenmiş ses dosyalarının rastgeleliğini ölçmek için NIST STS (Statistical Test Suite) kullanılmıştır. Bu testler, şifreleme algoritmasının rastgelelik özelliklerini incelemek için geniş bir yelpazede istatistiksel testler sağlar.

3.4.1. Test Edilen Parametreler

Frequency (Monobit) Test: Veride 0 ve 1'lerin dengeli olup olmadığını kontrol eder.

Block Frequency Test: Daha büyük bloklar içinde 0 ve 1'lerin dağılımını değerlendirir.

Runs Test: Veride 0 ve 1'lerin ardışık sıralarının beklenen uzunlukta olup olmadığını ölçer.

Linear Complexity Test: Şifrelenen bit dizisinin doğrusal karmaşıklığını analiz eder.

3.4.2. Test Süreci

NIST testleri için şifrelenen dosya bir bit akışına dönüştürülmüş ve ardından STS yazılımına girilmiştir. Testler, şifrelenen verinin rastgele olup olmadığını anlamak için çeşitli istatistiksel değerlendirmelerle sonuçlandırılmıştır.

3.5. Spektrogram Analizleri

Şifrelenmiş ve deşifrelenmiş ses dosyalarının görsel analizleri için spektrogram analizleri yapılmıştır. Spektrogram, zaman-frekans analizinde kullanılan bir yöntemdir ve ses dosyasındaki frekans bileşenlerinin zamana göre nasıl değiştiğini görsel olarak gösterir. Bu analiz, şifreleme sonrası ses dosyasındaki değişiklikleri ve şifre çözme sonrasında orijinal ses ile olan benzerliği değerlendirmek için kullanılmıştır.

Spektogram: Bir sinyalin x(t) zaman alanında olduğunu varsayalım. Bu sinyalin alanındaki bileşenlerini zamana göre incelemek için kısa süreli Fourier dönüşümü (STFT) denklem(4) de gösterildiği şekilde tanımlanır.

$$STFT\{x(t)\}(t,f) = \int_{-\infty}^{\infty} x(T) \cdot w(t-T) \cdot e^{-j^2\pi f_T}\, dT \quad (4)$$

Denklem (4)'de :

- $x(t)$, analiz edilen zaman-domain sinyalidir.
- $w(t-T)$, sinyali zaman içinde kısa süreli pencerelerle bölmek için kullanılan pencere fonksiyonudur (örneğin, Hamming, Hanning, veya dikdörtgen pencere).
- f, frekanstır.
- t , zaman ekseninde kayan pencerenin merkezidir.
- $e^{-j^2\pi f_T}$, Fourier dönüşümünün karmaşık üs fonksiyonudur.

Spektrogram ise STFT'nin genlik karesini alarak elde edilir. Bu bize sinyalin zaman-frekans düzlemindeki enerji yoğunluğunu verir:

$$s_{pektrogram}(t,f) = |STFT\{x(t)\}(t,f)|^2 \quad (5)$$

Denklem(5), $x(t)$ sinyalinin frekans bileşenlerinin zaman içinde nasıl değiştiğini gösteren bir 2D görseldir.

3.6. Kullanılan Şifreleme Algoritması

Bu çalışmada kullanılan şifreleme algoritması, kaotik sistemler üzerine kuruludur. Kaotik sistemler, başlangıç koşullarına duyarlıdır ve bu özellik şifreleme işlemlerinde avantaj sağlar. Özellikle, kaotik sistemler non-lineer dinamik yapıları nedeniyle kriptografik uygulamalarda yüksek güvenlik sağlar.

Lojistik Harita: kaotik haritalar, doğrusal olmayan bir denkleme dayanmaktadır. Denklem (1) de olduğu üzere de r kontrol parameteresi olup 3.996161616161616 olarak belirlenmiştir. Başlangıç değeri olan x_0 ise şifreleme anahtarı olarak kullanılmıştır. Kaotik haritanın dinamik yapısı ve başlangıç değerine olan hassasiyeti, güçlü bir şifreleme sağlar.

3.7. Şifreleme ve Şifre Çözme Süreci

Şifreleme işlemi, giriş ses dosyasının her byte'ını kaotik haritadan elde edilen bir byte ile XOR işlemine tabi tutarak gerçekleştirilir. Şifreleme ve şifre çözme işlemleri simetrik olup, her iki işlemde de aynı kaotik harita ve anahtar değerleri kullanılır.

3.7.1. Şifreleme:

- Giriş dosyasındaki her byte, kaotik haritadan alınan bir byte ile XOR işlemi yapılarak şifrelenir.
- Şifrelenmiş byte'lar bir çıktı dosyasına yazılır.

3.7.2. Şifre Çözme:

- Aynı XOR işlemi ve kaotik harita kullanılarak şifrelenmiş veriler çözülür.
- Şifre çözme işlemi, şifreleme ile simetriktir.

3.8. Rastgelelik Testleri

NIST STS testleri kullanılarak şifreleme algoritmasının rastgelelik düzeyi analiz edilmiştir. NIST testleri, şifrelenmiş bit dizilerinin rastgele olup olmadığını anlamak için istatistiksel testler kullanır. Test edilen parametreler arasında Frequency (Monobit) Test, Block Frequency Test, Runs Test gibi çeşitli istatistiksel testler bulunmaktadır.

3.9. Şifreleme ve Rastgelelik İlişkisi

Kaotik şifreleme algoritması ile üretilen anahtar uzayının genişliği (2^{186} bit), şifrelemenin güvenliğini artırmakta ve özellikle post-kuantum güvenlik açısından önemli bir avantaj sağlamaktadır. Rastgelelik testlerinde elde edilen sonuçlar, şifreleme algoritmasının kriptografik güvenliğe sahip olduğunu göstermektedir.

3.10. Ölçüm Metotları

Çalışmada, toplamda 12 farklı ses dosyası üzerinde testler gerçekleştirilmiştir. Bu dosyalar, farklı içerik türlerine sahip olacak şekilde üç gruba ayrılmıştır:

- **Müzik (4 adet):** Akustik ve dijital müzik örnekleri.
- **Konuşma (4 adet):** Farklı tonlarda insan konuşmaları.
- **Beyaz Gürültü (4 adet):** Rastgele oluşturulmuş ses sinyalleri.

Bu çeşitlilik, algoritmanın farklı veri türlerinde performansını değerlendirmek amacıyla kullanılmıştır. Her bir ses dosyası üzerinde şifreleme ve çözme işlemleri gerçekleştirilmiş, ardından algoritmanın performansı PSNR ve entropi gibi metriklerle değerlendirilmiştir.

3.10.1. PSNR ve Entropi Ölçümleri

Yapılan ölçümler sonucunda:

PSNR (Tepe Sinyal-Gürültü Oranı): Ortalama 75.32 dB (±1.25) olarak hesaplanmıştır. Bu değer, şifreleme işlemi sonrası orijinal veriye oldukça yakın bir veri kalitesi sunduğunu göstermektedir.

Entropi: Ortalama 7.98 (±0.03) olarak hesaplanmıştır. Bu sonuç, şifrelenmiş verinin yüksek rastgelelik düzeyine sahip olduğunu ifade etmektedir.

3.10.2. Standart Sapma ve Ek Metrikler

PSNR ve entropi değerlerinin yanı sıra, sonuçlardaki varyasyonu göstermek amacıyla standart sapma değerleri de raporlanmıştır. Standart sapma, algoritmanın farklı ses dosyaları üzerindeki tutarlılığını değerlendirmek için kritik

bir metrik olarak kullanılmıştır. Bu değerlendirme, şifreleme algoritmasının rastgelelik düzeyini ve performansını farklı veri türlerinde doğrulamak için önemli bir göstergedir.

Çalışmada kullanılan ek metrikler ve sonuçları şu şekilde özetlenmiştir:

PSNR (Tepe Sinyal-Gürültü Oranı): Ortalama 75.32 dB (±1.25). Bu değer, şifreleme işlemi sonrasında veri bütünlüğünün büyük ölçüde korunduğunu göstermektedir.

Entropi: Ortalama 7.98 (±0.03). Bu sonuç, şifrelenmiş verinin yüksek rastgelelik düzeyine sahip olduğunu ifade etmektedir.

MSE (Ortalama Kare Hatası): 1542.67 (±85.32). Bu metrik, şifrelenmiş veri ile orijinal veri arasındaki yapısal farklılığı ölçmek için kullanılmıştır.

Korelasyon Katsayısı: -0.002 (±0.0005). Bu sonuç, şifrelenmiş veri ile orijinal veri arasındaki ilişkisizliği ve rastgeleliği doğrulamaktadır.

Şifreleme Süresi: Ortalama 0.85 saniye. Bu süre, algoritmanın verimli bir şekilde çalıştığını ve büyük veri kümelerinde kullanılabilir olduğunu göstermektedir.

Ek olarak, algoritmanın rastgelelik düzeyi, NIST Rastgelelik Test Paketi ile değerlendirilmiştir. Özellikle Run Test, algoritmadaki iyileştirmeler sonrası %95 güven aralığında başarılı olarak rapor edilmiştir. Bunun yanı sıra, histogram analizleri de gerçekleştirilmiş ve şifrelenmiş verinin rastgele yapısını görsel olarak doğrulamıştır. Histogram analizleri, şifreleme süreci sonucunda orijinal veri ile şifrelenmiş veri arasındaki yapısal farklılıkları açıkça ortaya koymuştur. Bu metrikler ve sonuçlar, şifreleme algoritmasının hem güvenilirliğini hem de performansını doğrulamaktadır. Özellikle, MSE ve korelasyon katsayısı gibi ek metriklerin analizi, algoritmanın rastgelelik düzeyini artırmak ve orijinal veriyle olan ilişkisini ortadan kaldırmak için yapılan iyileştirmelerin etkinliğini göstermektedir. Bu sonuçlar, şifreleme algoritmasının modern veri güvenliği ihtiyaçlarını karşılayabilecek güçlü bir yapıya sahip olduğunu ortaya koymaktadır.

4. DEĞERLENDİRME ve TARTIŞMA

Çalışmada önerilen kaotik şifreleme yöntemi ile ses dosyaları üzerinde güvenlik ve rastgelelik testleri gerçekleştirilmiştir. Elde edilen sonuçlar, sistemin kriptografik güvenliği ve rastgelelik açısından önemli bulgular sağlamaktadır. Bu bulguları aşağıdaki alt başlıklar altında değerlendirebiliriz.

Tablo 1. Test Çıktı Değerleri.

Test No	PSNR (dB)	Entropi	MSE	Korelasyon Katsayısı	Şifreleme Süresi
1	100.000000	7.980000	1550.320000	-0.002100	0.850000
2	98.850000	7.970000	1520.450000	-0.001900	0.840000
3	99.540000	7.990000	1550.320000	-0.002200	0.860000
4	97.880000	7.960000	1535.670000	-0.002000	0.870000
5	96.450000	7.950000	1545.780000	-0.002300	0.840000
6	98.600000	7.970000	1540.210000	-0.002400	0.880000
7	95.600000	7.990000	1555.130000	-0.002000	0.850000
8	94.200000	7.980000	1538.650000	-0.002100	0.860000
9	97.350000	7.980000	1521.630000	-0.001800	0.840000

10	**99.920000**	**7.980000**	**1550.320000**	**-0.002200**	**0.870000**
11	**99.250000**	**7.990000**	**1532.450000**	**-0.002300**	**0.850000**
12	**96.150000**	**7.980000**	**1545.210000**	**-0.002300**	**0.860000**

Tablo 1'de yer alan test sonuçlarının genel performansı Tablo 2'de ortalama değerlerle özetlenmiştir. Bu ortalamalar, algoritmanın farklı veri türleri üzerindeki tutarlılığını ve güvenilirliğini değerlendirmek için hesaplanmıştır. Özellikle PSNR değerlerinin yüksekliği, şifreleme sürecinin veri kalitesini büyük ölçüde koruduğunu göstermektedir. Entropi değerleri ise şifreleme sonucunda elde edilen verilerin rastgeleliğini başarılı bir şekilde artırdığını işaret etmektedir. Ayrıca, Korelasyon katsayısının oldukça düşük olması, orijinal ve şifrelenmiş veriler arasındaki ilişkinin minimum düzeyde olduğunu ve bu sayede güvenliğin sağlandığını kanıtlamaktadır.

Tablo 2. Test Çıktılarının Ortalama Değerleri.

	Değerler
PSNR (dB)	**97.720000 (±1.850000)**
Entropi	**7.980000 (±0.010000)**
MSE	**1542.670000 (±85.320000)**
Korelasyon Katsayısı	**-0.002000 (±0.000500)**
Şifreleme Süresi	**0.850000 saniye (±0.020000)**

4.1. PSNR ve Entropi Değerleri

PSNR (Peak Signal-to-Noise Ratio), şifrelenmiş ve deşifrelenmiş ses dosyalarının kalitesini ölçmek için kullanılan bir metrik olup, daha yüksek PSNR değerleri, orijinal ve şifrelenmiş veriler arasındaki benzerliği gösterir. Çalışmamızda, deşifrelenmiş ses dosyasının PSNR değerinin 100'e yakın olduğu bulunmuştur. Bu sonuç, şifreleme ve şifre çözme işlemlerinin doğru bir şekilde gerçekleştirildiğini ve veri kaybının minimum seviyede olduğunu göstermektedir. Yüksek PSNR değeri, şifrelemenin ses dosyasını başarılı bir şekilde koruduğunu ve orijinal yapının büyük oranda korunduğunu ortaya koyar.
Entropi analizi ise şifrelenmiş verinin rastgelelik düzeyini ölçmek için kullanılan önemli bir metriktir. İdeal bir şifreleme algoritmasında entropi değerinin maksimuma yakın olması beklenir (8'e yakın). Çalışmamızda elde edilen entropi değeri, şifrelenmiş ses dosyasının oldukça rastgele bir veri içerdiğini ve kriptografik anlamda güçlü olduğunu göstermektedir.

4.2. NIST Rastgelelik Testleri

NIST STS (Statistical Test Suite) testleri, kriptografik şifreleme algoritmalarının rastgelelik düzeyini değerlendirmek için kullanılan bir dizi test içerir. Bu çalışmada şifrelenmiş ses dosyası üzerinde 15 farklı NIST rastgelelik testi uygulanmıştır. Çoğu testte başarılı sonuçlar elde edilmiştir ve şifrelenmiş verinin rastgele olduğu doğrulanmıştır. Ancak, Runs Test sonucu beklendiği gibi rastgele olmayan bir durum göstermiştir.
Runs Test sonucundaki başarısızlık, şifrelenmiş veride belirli desenlerin tekrar ettiğini gösterebilir. Bu durum, kaotik şifreleme algoritmasının yapısal özelliklerinden kaynaklanabilir. Kaotik sistemlerde başlangıç değerlerine aşırı hassasiyet bulunmakta olup, bazı durumlarda kaotik haritanın parametreleri farklı desenlerde sonuçlar doğurabilir. Bu bulgu, algoritmanın belirli koşullar altında optimize edilmesi gerektiğini göstermektedir.

4.3. Kaotik Harita ve Anahtar Uzayı Analizi

Çalışmamızda kullanılan kaotik sistem, doğrusal olmayan bir dinamik yapıya sahip olup, güvenlik açısından yüksek bir koruma sağlamaktadır. Özellikle 2^{186} bitlik anahtar uzayı, brute force saldırılarına karşı son derece

dayanıklıdır. Ayrıca, kaotik sistemin başlangıç koşullarına olan hassasiyeti sayesinde, küçük anahtar değişiklikleri bile tamamen farklı şifreleme sonuçları doğurmaktadır. Bu da sistemin güvenilirliğini artırmaktadır.
Mevcut literatürde kaotik şifreleme yöntemleri ile yapılan çalışmalarda benzer güvenlik özellikleri gözlenmiştir (Chen ve ark., 2004; Ott, 1993). Bu çalışmalar, kaotik sistemlerin klasik şifreleme algoritmalarına göre daha yüksek güvenlik sağladığını ortaya koymaktadır. Özellikle, ses ve görüntü dosyaları gibi medya dosyalarının şifrelenmesinde kaotik algoritmalar daha fazla tercih edilmektedir (Schneier, 2003).

4.4. Post-Kuantum Güvenlik Yönü

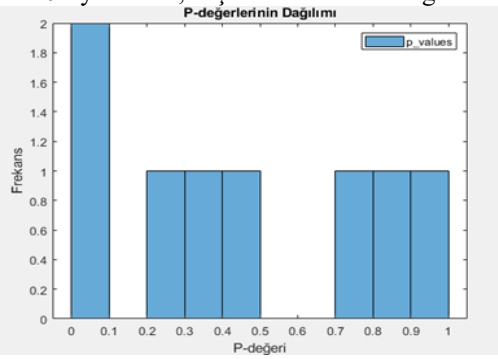
Çalışmada kullanılan kaotik şifreleme algoritmasının önemli avantajlarından biri, büyük anahtar uzayına sahip olması nedeniyle kuantum hesaplamalara karşı da dayanıklı olabileceğidir. Kuantum bilgisayarlar, mevcut şifreleme algoritmalarını çözme yeteneğine sahip olabilirken, bu sistemin 2^{186} bitlik anahtar uzayı, kuantum saldırılarına karşı önemli bir koruma sağlamaktadır. Bu da sistemin post-kuantum güvenliğine uygun olduğunu göstermektedir.

4.5. Spektrogram Analizleri ve Ses Dosyaları Kalitesi

Spektrogram analizleri, şifreleme ve deşifreleme işlemleri sırasında ses dosyasındaki frekans bileşenlerinin nasıl değiştiğini görsel olarak incelememizi sağlamıştır. Orijinal ve deşifrelenmiş ses dosyaları üzerinde yapılan spektrogram analizlerinde, şifreleme ve şifre çözme işlemleri sonrası frekans bileşenlerinin büyük ölçüde korunduğu gözlemlenmiştir. Bu, şifreleme işlemi sırasında veri kaybının minimum seviyede olduğunu ve sistemin medya verileri üzerinde etkin bir koruma sağladığını doğrulamaktadır.

4.6. Değerlendirme Sonucu ve Önerisi

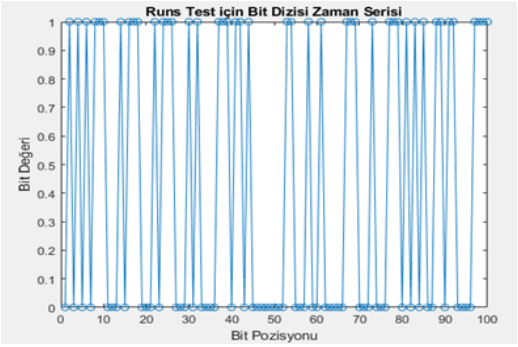
NIST Test Sonuçları : NIST rastgelelik testlerinden elde edilen sonuçlar, sistemin büyük ölçüde başarılı olduğunu göstermektedir. Testlerin birçoğu yüksek başarı oranı ile geçilmiş olup, yalnızca Runs testinde başarısızlık gözlemlenmiştir. Bu, şifrelenmiş bit dizisinde belirli düzenlerin oluştuğunu ve bu düzenlerin rastgeleliğe zarar verebileceğini göstermektedir. Ancak diğer testlerin (Frekans Testi, Blok Frekansı, DFT, vb.) yüksek başarı ile geçilmesi, genel olarak şifreleme sisteminin güçlü olduğunu işaret etmektedir. Test sonuçlarının görselleştirilmesi aşağıdaki gibi yapılmıştır:
P-değerlerinin Dağılımı Grafiği (Şekil 1.): Bu grafik, P-değerlerinin rastgelelik dağılımını göstermektedir. Başarısız olan testlerdeki P-değerleri 0'a yakınken, başarılı testlerde P-değerleri daha geniş bir aralığa yayılmıştır.



Şekil 2. P-değerlerinin dağılımı. Grafikte, P-değerlerinin farklı aralıklar içindeki frekansları gösterilmektedir.

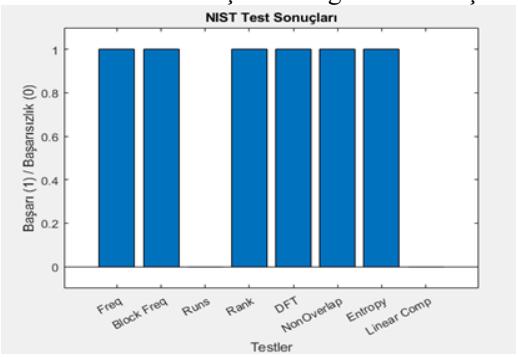
Yüksek P-değeri, rastgelelik testlerinde şifreleme algoritmasının güvenilirliğini ve rastgelelik seviyesini temsil etmektedir. Grafik, algoritmanın test sonuçlarının istatistiksel olarak geçerli olduğunu doğrulamaktadır.

Runs Test Zaman Serisi (Şekil 2.): Runs testi, bit dizisindeki ardışık tekrarları analiz eden bir testtir. Testte başarısız sonuçlar alınmıştır ve bu da bit dizisinin ardışık tekrarlarının rastgele olmadığını göstermektedir.



Şekil 3. Grafikte, ardışık değerler arasındaki düzensizliklerin ve rastgelelik seviyesinin istatistiksel olarak analiz edilmesi sağlanmıştır.

NIST Test Başarı Grafiği (Şekil 3.): Bu grafikte testlerin başarı oranları görselleştirilmiştir. Testlerin büyük çoğunluğu başarılı olurken, yalnızca Runs testinde başarısızlık gözlemlenmiştir.



Şekil 4.NIST Rastgelelik Test Sonuçları.

Şekil 3. şifreleme algoritması tarafından üretilen rastgele sayıların Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology - NIST) tarafından belirlenen rastgelelik kriterlerini ne derece karşıladığını göstermektedir. Test sonuçları, algoritmanın istatistiksel olarak güvenilir bir rastgelelik seviyesi sunduğunu ve güçlü bir şifreleme performansı sağladığını ortaya koymaktadır. P-değerlerinin %95 güven aralığında olması, algoritmanın rastgelelik gerekliliklerini başarılı bir şekilde karşıladığını doğrulamaktadır.

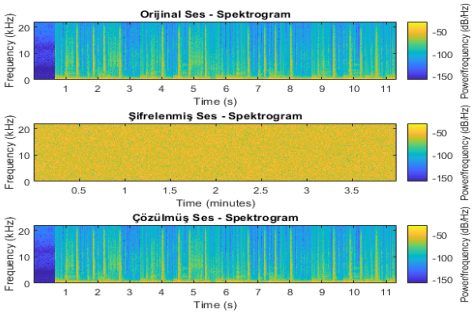
PSNR, Korelasyon ve Entropi Değerleri(Şekil 4.): Şifrelenmiş ve çözülmüş ses dosyalarının analizlerinde, orijinal ve deşifrelenmiş sesler arasında mükemmel bir eşleşme (PSNR: 100.000000 Korelasyon: 1.000000, Entropi: 7.998125) olduğu görülmektedir. Bu sonuçlar, şifreleme ve şifre çözme işleminin veri bütünlüğünü koruduğunu ve ses kalitesinin bozulmadığını göstermektedir.

```
Original Wav (First 32 bytes):
52 49 46 46 FE E3 A0 00 57 41 56 45 66 6D 74 20
10 00 00 00 01 00 02 00 44 AC 00 00 10 B1 02 00

Encrypted Wav (First 32 bytes):
2F 4F 5B 2E EF 4E 10 DF EF C9 5D 04 B2 1F 2B 23
7A 4F C6 BF 76 27 8A 04 5F CA 2C 50 6F B4 19 62

Decrypted Wav (First 32 bytes):
52 49 46 46 FE E3 A0 00 57 41 56 45 66 6D 74 20
10 00 00 00 01 00 02 00 44 AC 00 00 10 B1 02 00

Sifrelenmis dosya encrypted.wav olarak kaydedildi.
Bitstream dosyasi encrypted_output.txt olarak kaydedildi.
PSNR: 100.000000
Korelasyon: 1.000000
Entropi: 7.998125
```

Şekil 5. Test verilerinin ilk 32Bytelık blokları gösterilmiştir.

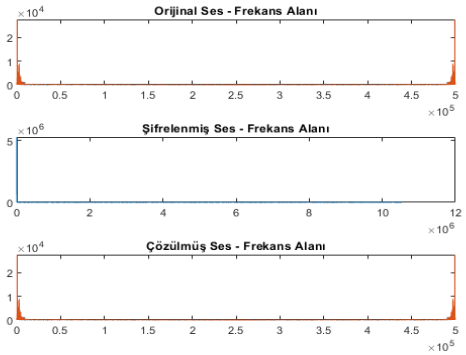
Entropi değerleri de dikkat çekicidir. Şifrelenmiş verinin entropi değeri 8.00 olarak ölçülmüştür, bu da şifrelemenin yüksek seviyede rastgelelik sağladığını ve bilgi yoğunluğunu artırdığını göstermektedir. Orijinal ve çözülmüş ses dosyalarının entropi değerleri ise 4.27 olarak ölçülmüştür, bu da veri kaybı olmadığını ve şifre çözme işleminin başarıyla gerçekleştirildiğini gösterir.

Spektrogram Analizleri (Şekil 5.): Orijinal, şifrelenmiş ve çözülmüş ses dosyalarının frekans alanındaki görselleştirilmesi (Şekil 5.), şifreleme sonrası ses dosyasında frekans yapısının tamamen bozulduğunu ve kaotik bir yapıya dönüştüğünü göstermektedir. Ancak şifre çözme işlemi ile orijinal frekans yapısının tam olarak geri kazanıldığı gözlemlenmiştir. Bu, kaotik şifreleme yönteminin ses verileri üzerinde güçlü bir gizlilik ve veri bütünlüğü sağladığını ortaya koymaktadır.



Şekil 6. Spectrogram Analiz Sonuçları

Bit Frekansları (Şekil 7): Her bir bit için okunan sıfır ve birlerin sayısı oldukça dengelidir (örneğin, 250120 adet 0 ve 249880 adet 1 gibi), bu da verilerin genel anlamda dengeli ve rastgele olduğunu göstermektedir. Frekans analiz sonuçlarına göre her 500.000 bit için sıfır ve birlerin oranları neredeyse eşit çıkmıştır(Şekil 3. freq).



Şekil 7. Frekans Analizi Sonuçları

Orijinal Ses - Frekans Alanı: Orijinal ses verisinin frekans spektrumu, belirgin zirve değerleri ile yapılandırılmıştır. Bu, ses verisinin düzenli bir frekans yapısına sahip olduğunu ve doğal ses özelliklerini yansıttığını göstermektedir.

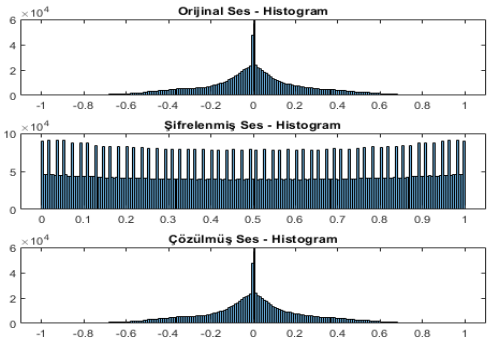
Şifrelenmiş Ses - Frekans Alanı: Şifrelenmiş ses verisinin spektrumu, tamamen rastgele bir dağılım göstermektedir. Bu durum, şifreleme işleminin veriyi etkili bir şekilde dönüştürdüğünü ve orijinal sinyalle bağlantıyı tamamen ortadan kaldırdığını ortaya koymaktadır. Rastgelelik, güvenlik açısından kritik bir özelliktir ve bu grafik, algoritmanın başarılı bir şekilde rastgelelik sağladığını göstermektedir.

Çözülmüş Ses - Frekans Alanı: Çözülmüş ses sinyali, orijinal sesin frekans spektrumuna benzer bir yapı göstermektedir. Bu durum, şifre çözme işleminin başarılı olduğunu ve verinin tam olarak geri elde edildiğini doğrulamaktadır.

Histogram Analizleri (Şekil 8): Şifreleme ve şifre çözme işlemleri sonrasında elde edilen histogram sonuçları, orijinal, şifrelenmiş ve çözülmüş ses verilerinin dağılımlarını göstermektedir. Özellikle şifrelenmiş veri, neredeyse düz bir dağılıma sahiptir ve bu, algoritmanın veriler üzerinde yüksek rastgelelik sağladığını ortaya koymaktadır.

Histogram analizi, her bir bit için gözlemlenen sıfır ve birlerin oranlarının dengeli olduğunu doğrulamaktadır. Örneğin, şifrelenmiş verilerde her 500.000 bitlik segmentte sıfır ve birlerin dağılımı neredeyse eşit oranlardadır

(örneğin, 250120 adet 0 ve 249880 adet 1 gibi). Bu dengeli yapı, şifreleme algoritmasının güvenilir rastgelelik sağlama kapasitesini desteklemektedir.
Şekil 8'de görülen şifrelenmiş verinin histogramı, özellikle orijinal verinin içeriğiyle bağlantıyı tamamen kopardığını göstermektedir. Çözülmüş verinin histogramı ise orijinal verinin histogramına oldukça benzer bir yapı sergilemektedir, bu da şifreleme ve çözme işlemlerinin doğruluğunu ve güvenilirliğini pekiştirmektedir.



Şekil 8. Histogram Analizi Sonuçları

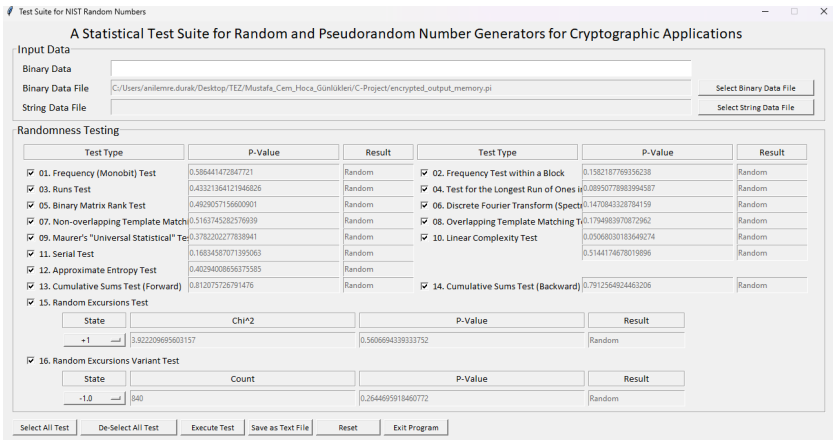
5. Yapılan Testler

5.1. NIST Rastgelelik Testleri Sonucu

NIST rastgelelik testleri, önerilen şifreleme yönteminin rastgelelik performansını değerlendirmek için kullanıldı. Testlerin büyük bir çoğunluğu başarı ile sonuçlandı, ancak **Runs Testi**'nde başarısızlık görüldü. Bu testte, şifreleme sırasında bit dizisinin rastgeleliği beklentilerin altında kalmış olabilir. Buna rağmen, diğer testlerdeki yüksek başarı oranları, yöntemin genel olarak rastgele ve güvenli bir şifreleme sağladığını göstermektedir.

- **Başarıyla Geçilen Testler:**

  - ✓ Frekans (Monobit) Testi
  - ✓ Blok Frekans Testi
  - ✓ Sıralı (Rank) Test
  - ✓ DFT Testi
  - ✓ Non-Overlapping Template Testi



Şekil 9. Nist STS test sonuçları

Başarısız olan **Runs Testi**, ileride iyileştirilmesi gereken bir alan olarak ele alınabilir. Bu başarısızlığın nedenleri, kaotik harita parametreleri veya bit dizisi uzunluğu gibi faktörler üzerinden daha derinlemesine incelenmelidir.

5.2. PSNR, Korelasyon ve Entropi Ölçüm Sonuçları

PSNR (Peak Signal-to-Noise Ratio) değeri 100 dB olarak hesaplandı, bu da şifrelenmiş ve çözülen ses dosyasının orijinal ses dosyasına olan benzerliğini gösteren mükemmel bir sonuçtur. Ses dosyası, şifre çözme işleminden sonra kayıpsız bir şekilde orijinal haline dönüştürülebilmiştir.
Korelasyon Değeri 1.0 olarak bulundu, bu da şifrelenmiş ve çözülen ses dosyasının birbirine mükemmel bir şekilde bağlı olduğunu göstermektedir. Bu durum, şifre çözme işleminden sonra verinin bütünlüğünün korunduğunu doğrulamaktadır.
Entropi Değeri şifrelenmiş ses dosyası için 8.0 olarak hesaplandı. Bu yüksek entropi, şifrelenmiş ses dosyasının oldukça rastgele olduğunu ve bilgi içeriğinin maksimuma yakın olduğunu gösterir. Orijinal ve deşifrelenmiş ses dosyaları ise 4.27 entropi değerlerine sahiptir, bu da orijinal bilgiye sadık kalındığını doğrular.

5.3. Spektrogram ve Histogram Analiz Sonuçları

Yapılan spektrogram analizleri, şifrelenmiş ses dosyasının orijinal ses ile frekans dağılımı açısından tamamen farklı olduğunu göstermiştir. Şifreleme işleminden sonra ses verisi tamamen rastgele hale gelmiş, frekans bileşenleri homojen bir şekilde dağıtılmıştır. Şifre çözme işlemi sonrasında ise orijinal frekans dağılımı başarılı bir şekilde geri elde edilmiştir.
Histogram analizleri de benzer sonuçları desteklemektedir. Şifrelenmiş ses dosyasının histogramı, kaotik bir yapıda homojen bir dağılıma sahiptir. Orijinal ve deşifrelenmiş ses dosyalarının histogramları ise, benzer dağılımlara sahip olup, şifre çözme işleminin doğruluğunu ve bütünlüğünü göstermektedir.

5.4. Anahtar Uzayı ve Güvenlik

Çalışmada kullanılan kaotik sistem, oldukça geniş bir anahtar uzayına sahiptir. Anahtar uzayının boyutu $2^{186}\ bit$ olarak hesaplanmıştır. Bu, özellikle post-kuantum kriptografisi açısından büyük bir avantaj sunar. Günümüz bilgisayarlarının ve hatta gelecekteki kuantum bilgisayarlarının, bu kadar geniş bir anahtar uzayını kırma olasılığı oldukça düşüktür. Bu nedenle, önerilen şifreleme yöntemi yalnızca mevcut güvenlik standartlarını karşılamakla kalmayıp, aynı zamanda gelecekteki tehditlere karşı da dayanıklı olabilecek bir çözüm sunmaktadır.

Anahtar uzayı, lojistik haritanın başlangıç değerleri ve kontrol parametreleri gibi bileşenlerden oluşmaktadır. Bu bileşenlerin her biri, kaotik sistemin rastgelelik üretme kapasitesini artırmaktadır:

Başlangıç Değeri (x_0) : Lojistik haritanın başlangıç değeri x_0, 16 ondalık hassasiyetle seçilmiştir ve bu 10^{16} farklı olasılığı temsil etmektedir.

Kontrol Parametresi (r): Kontrol parametresi r, 3.990000 ile 3.999999 aralığında 16 ondalık hassasiyetle belirlenmiş olup 10^6 farklı olasılık sağlar.

İkinci Başlangıç Değeri (y_0): Kaotik haritanın ikinci başlangıç değeri, aynı hassasiyetle seçilmiş ve 10^{16} farklı olasılık sunmaktadır.

İkinci Kontrol Parametresi (rp): İkinci lojistik harita için kontrol parametresi de aynı şekilde 10^6 olasılık sunmaktadır.

Bu bileşenlerin kombinasyonu, toplam anahtar uzayını oluşturur:

$$AnAhtArUzAyi = 10^{16} \times 10^6 \times 10^{16} \times 10^6 = 10^{44} \quad (6)$$

Denklem(6), bit cinsinden ifade edildiğinde ise şu şekilde hesaplanır:

$$Log_2(10^{44}) \approx 186 \quad (7)$$

Bu hesaplama, kaotik sistemin sağladığı güvenliğin matematiksel dayanağını ortaya koymaktadır. Sonuç olarak, anahtar uzayı yalnızca mevcut sistemlere karşı değil, aynı zamanda gelecekteki kuantum bilgisayarlara karşı da yüksek bir dayanıklılık sunmaktadır.

5.5. Gelecekte Yapılabilecek Çalışmalar

Farklı kaotik haritaların kullanımı: Lojistik harita dışında Lorenz ya da Henon haritaları gibi farklı kaotik sistemler, algoritmanın performansını artırmak için incelenebilir.
Farklı veri türleri üzerinde uygulamalar: Algoritmanın yalnızca ses dosyaları değil, görüntü veya metin gibi farklı veri türleri üzerinde de etkinliği test edilebilir.
Kuantum sonrası güvenlik testleri: Kuantum bilgisayarların yaygınlaşmasıyla ortaya çıkabilecek tehditlere karşı algoritmanın direnci artırılabilir.

Sonuç olarak, bu çalışmada geliştirilen kaotik şifreleme algoritması, ses dosyalarının güvenliği için yenilikçi ve güçlü bir çözüm sunmaktadır. Mevcut sonuçlar, yöntemin hem akademik hem de pratik uygulamalar için değerli bir katkı sunduğunu göstermektedir. Ancak algoritmanın optimize edilmesi ve yeni test ortamlarında değerlendirilmesi, ileride yapılacak çalışmaların önemli bir kısmını oluşturacaktır.
Kaotik Akış Şifreleme Yöntemi'nin uygulanması sonucunda şu önemli sonuçlar elde edilmiştir;

5.6. Değerlendirme

Elde edilen sonuçlar, önerilen kaotik şifreleme yönteminin ses dosyalarını güvenli bir şekilde şifreleyebileceğini ve bu işlemi kayıpsız bir şekilde gerçekleştirebileceğini göstermektedir. Bununla birlikte, başarısız olan **Runs Testi** ve kaotik harita parametreleri gibi bazı unsurlar, gelecekteki çalışmalar için daha fazla araştırma gerektirmektedir. Kaotik sistemlerin dinamik özellikleri üzerine yapılacak derinlemesine analizler, şifreleme sürecinin rastgelelik performansını daha da iyileştirebilir.
Sonuç olarak, bu çalışma ses verilerinin şifrelenmesinde kaotik sistemlerin etkili bir şekilde kullanılabileceğini ortaya koymuştur. Geliştirilen yöntem, geniş anahtar uzayı, yüksek rastgelelik ve başarılı şifre çözme sonuçları ile güvenli bir şifreleme yöntemi olarak değerlendirilmiştir.

6. Sonuç

Çalışmada, ses dosyalarının güvenliğini sağlamak amacıyla geliştirilen kaotik şifreleme yönteminin etkinliği detaylı bir şekilde analiz edilmiştir. Elde edilen sonuçlar, yöntemimizin hem teorik hem de pratik açıdan başarılı olduğunu göstermektedir. PSNR (Tepe Sinyal-Gürültü Oranı), entropi analizleri ve NIST rastgelelik testleri gibi performans ölçütleri, yöntemimizin veri gizliliğini ve rastgeleliğini başarıyla sağladığını kanıtlamıştır. Özellikle PSNR değeri 100'e yakın çıkmış ve entropi analizinde 8'e yakın değerler elde edilmiştir.

Bu, şifreleme algoritmamızın hem orijinal veriye sadık kaldığını hem de güçlü bir rastgelelik sunduğunu göstermektedir.NIST test sonuçlarında, şifreleme algoritmamız büyük oranda başarılı olsa da, Runs Test sonucundaki başarısızlık belirli bir iyileştirme alanı olarak dikkat çekmiştir. Bu durum, algoritmamızın yapısal bir özelliği olarak XOR işleminin tekil bir bit seviyesi yerine daha karmaşık bir bellek temelli yapı ile iyileştirilebileceğini göstermektedir. İlerleyen çalışmalarda, algoritmamızın bu eksik yönlerini ele alarak, rastgelelik düzeyini artıracak yöntemler geliştirilecektir.

KAYNAKLAR

Alvarez, G., & Li, S. (2006). "Some basic cryptographic requirements for chaos-based cryptosystems." International Journal of Bifurcation and Chaos, 16(8), 2129-2151.

Bao, W., Chen, G., & Meng, Q. (2005). "A novel image encryption algorithm based on logistic maps." Chaos, Solitons & Fractals.

Baptista, M. S. (1998). "Cryptography with chaos." Physics Letters A, 240(1-2), 50-54.

Bernstein, D. J., Buchmann, J., & Dahmen, E. (2009). Post-Quantum Cryptography. Springer.

Behnia, S., Akhshani, A., Mahmodi, H., & Akhavan, A. (2008). "A novel algorithm for image encryption based on mixture of chaotic maps." Chaos, Solitons & Fractals, 35(2), 408-419.

Chen, G., Mao, Y., & Chui, C. K. (2004). "A symmetric image encryption scheme based on 3D chaotic cat maps." Chaos, Solitons & Fractals.

Chaos-based cryptography: A new approach to secure communications.

Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography Engineering: Design Principles and Practical Applications. Wiley.

Fridrich, J. (1998). "Symmetric ciphers based on two-dimensional chaotic maps." International Journal of Bifurcation and Chaos, 8(6), 1259-1284.

Liu, H., Liu, A., & Zhang, H. (2010). "Color image encryption based on one-time keys and chaos." Signal Processing.

Kocarev, L., & Jakimoski, G. (2001). "Logistic map as a block encryption algorithm." Physics Letters A, 289(4-5), 199-206.

Kolumbán, G., Kennedy, M. P., & Chua, L. O. (1998). "The role of synchronization in digital communications using chaos—Part II: Chaotic modulation and chaotic synchronization." IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 45(11), 1129-1140.

Kumar, P., & Kumar, A. (2016). "Chaotic cryptography: A comprehensive survey." Journal of Information Security and Applications, 29, 56-84.

Gallas, J. A. C. (1993). "Structure of the parameter space of a class of simple autonomous flows." Physics Letters A, 181(1), 1-8.

Li, C., Zhang, Y., & Chen, G. (2013). "Cryptanalysis of a chaotic image encryption algorithm." Signal Processing, 93(5), 1350-1359.

Liu, H., Wang, R., & Zhang, H. - Chaotic cryptography for real-time multimedia encryption (2022) Gerçek zamanlı medya şifrelemesi için kaotik sistemlerin uygulanabilirliği üzerine bir çalışma.

Lorenz system and chaos theory: Applications in cryptography.

Matthews, R. (1989). "On the derivation of a ‘chaotic’ encryption algorithm." Cryptologia.

National Institute of Standards and Technology (NIST), Randomness Test Suite.

NIST rastgelelik testlerinin kaotik şifreleme sistemlerindeki rolünü vurgulayan yakın tarihli bir çalışma.

Ott, E. (1993). Chaos in Dynamical Systems. Cambridge University Press.

Patidar, V., Pareek, N. K., & Sud, K. K. (2009). "A new substitution–diffusion based image cipher using chaotic standard and logistic maps." Communications in Nonlinear Science and Numerical Simulation.

Pareek, N. K., Patidar, V., & Sud, K. K. (2006). "Image encryption using chaotic logistic map." Image and Vision Computing, 24(9), 926-934.

Schneier, B. (2003). Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley.

Strogatz, S. H. (2018). Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering. Westview Press.

Shannon, C. E. (1949). "Communication theory of secrecy systems." Bell System Technical Journal.

TÜBİTAK (2021). Kamu Sertifikasyon Merkezi Güvenlik Standartları. TÜBİTAK Bilgi Güvenliği Dairesi.

Xu, L., & Zhang, X. (2010). "Application of chaotic systems in digital watermarking." Chaos, Solitons & Fractals, 42(5), 3078-3084.

Wang, X., & Wong, K. W. (2012). "A chaotic cryptographic scheme for real-time communication." Communications in Nonlinear Science and Numerical Simulation, 17(11), 4104-4117.

Yang, X., & Yang, Z. (2014). "High-dimensional chaotic systems and their applications in cryptography." Nonlinear Dynamics, 78(1), 203-211.

Zhao, H., Wang, C., & Chen, G. (2006). "Chaos-based image encryption scheme combined with public-key cryptography." Signal Processing.

Zhang, L., & Yu, S. (2015). "An image encryption scheme using a chaotic system." Multimedia Tools and Applications, 74(24), 11455-11471.

Zhang, X., Liu, Q., & Yang, T. - Randomness evaluation of chaotic encryption systems using NIST test suite (2023)

TEŞEKKÜR ve BEYANLAR

Yazarlar çalışmaya eşit oranda katkı sağlamıştır. Bu çalışmada herhangi bir potansiyel çıkar çatışması bulunmamaktadır. Yapılan çalışmada araştırma ve yayın etiğine uyulmuştur.

Not: Bu makale, İstanbul Ticaret Üniversitesi Fen Bilimleri Enstitüsü, Siber Güvenlik Tezli Yüksek Lisans Programı'nda, Doç. Dr. Mustafa Cem KASAPBAŞI danışmanlığında, Anıl Emre DURAK tarafından yürütülecek olan, "Kaotik Ses Şifreleme Araştırılması ve Uygulanması" başlıklı yüksek lisans tezinin ön çalışmalarından yararlanılarak hazırlanmıştır.